情報システム論

第7回

今日の話題

- Webの基本
- 暗号化

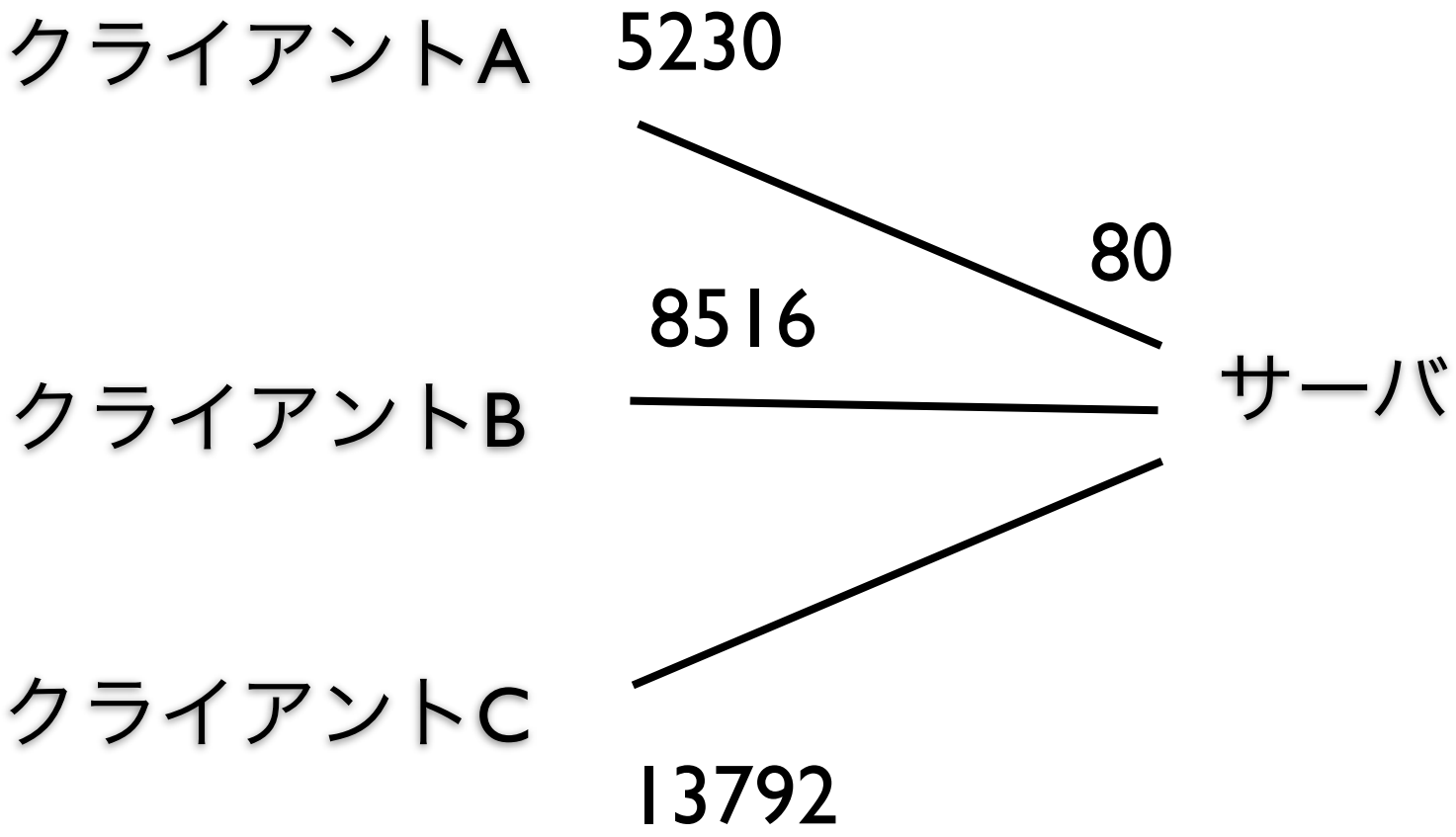
クライアント・サーバ

- サーバ
  - メールサーバ
    - POP、SMTP、IMAP
  - Webサーバ
  - ファイルサーバ

Well-known ポート

- 一般的なサービスで使用されるポート
  - TCP/22 SSH
  - TCP/23 Telnet
  - TCP/25 SMTP
  - TCP/80 HTTP
  - TCP/110 POP3
  - TCP/143 IMAP
  - TCP/443 HTTPS

クライアント・サーバ



World Wide Web

- 1990年 CERN (欧州原子核機構)で開発
- 1992年 NCSA (イリノイ大学　米国立スーパーコンピュータ応用研究所)でMosaicを開発
- 1993年 一般利用開始

Webを支える技術

- URI
  - リソース識別子
- HTTP
  - プロトコル
- HTML
  - 文書構造と内容

URI

- 統一資源識別子(Uniform Resource Identifier)
- 一定の書式によってリソース(資源)を指し示す識別子
- スキーム:スキームごとに定義された書式

URIの例

- http://www.kyushu-u.ac.jp/
- http://www.kyushu-u.ac.jp:80/student/
- https://sso.kyushu-u.ac.jp/
- http://jin:pass@jin-lab.jp/search?q=test
- mailto:jin@cc.kyushu-u.ac.jp
- urn:isbn:9783621411249

URIで使用できる文字

- http://ja.wikipedia.org/wiki/九州大学

- http://ja.wikipedia.org/%E4%B9%9D%E5%B7%9E%E5%A4%A7%E5%AD%A6

絶対URI、相対URI

- http://www.kyushu-u.ac.jp/
- http://www.kyushu-u.ac.jp/students/
- students
- ../img/log.gif

HTTP

- Hyper Text Transfer Protocol
- アプリケーション層

OSI参照モデル

Open Systems Interconnection

アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層

リクエストとレスポンス

- クライアント
  - リクエスト
- サーバ
  - レスポンス

リクエスト

GET / HTTP/1.1

Host: lss.ifs.kyushu-u.ac.jp

User-Agent: .....

Accept: text/html, ...

Accept-Language: ja, en-us,....

Accept-Charset: Shift_JIS, utf-8,...

レスポンス

HTTP/1.1 200 OK

Date: Tue, 17 Jun 2013 02:33:03 GMT

Server: Apache/2.2.9 (Fedora)

Transfer-Encoding: chunked

Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

メソッド

- GET: リソースの取得
- POST: リソースへのデータの追加
- HEAD: リソースのヘッダの取得
- PUT、DELETE、OPTIONS、TRACE、CONNECT

ステータス

- 200: OK
- 304: Not Modified
- 403: Forbidden
- 404: Not Found
- 500: Internal Server Error

HTML

- HyperText Markup Language
- タグで文章の構造を表現
- 構造化文書 (Structured Document)

HTMLの構成要素

```
<html>
    <head>
      <title>情報システム論</title>
    </head>
    <body>
        <h1>第7回</h1>
        <p>本日の授業では、...</p>
        <ul>
            <li>Webの基本</li>
        </ul>
        ......
    </body>
</html>
```

リンク

- 九州大学
- <img src=”logo.gif”>

情報伝達に関する技術

- 正確に伝達
- 機密的に伝達
- 発信元を保証
- 不要な情報を受信しない、発信しない

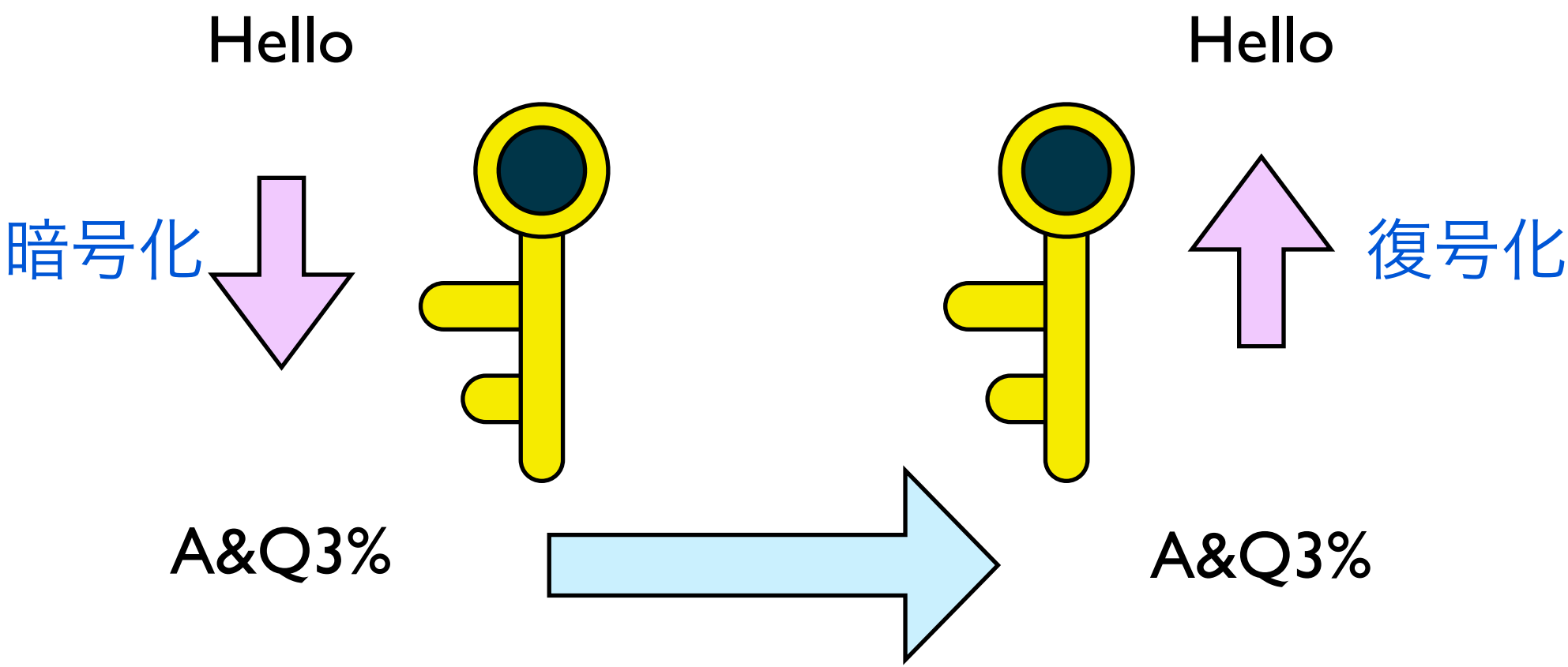
正確に伝達

- チェックサム
- シーケンス番号

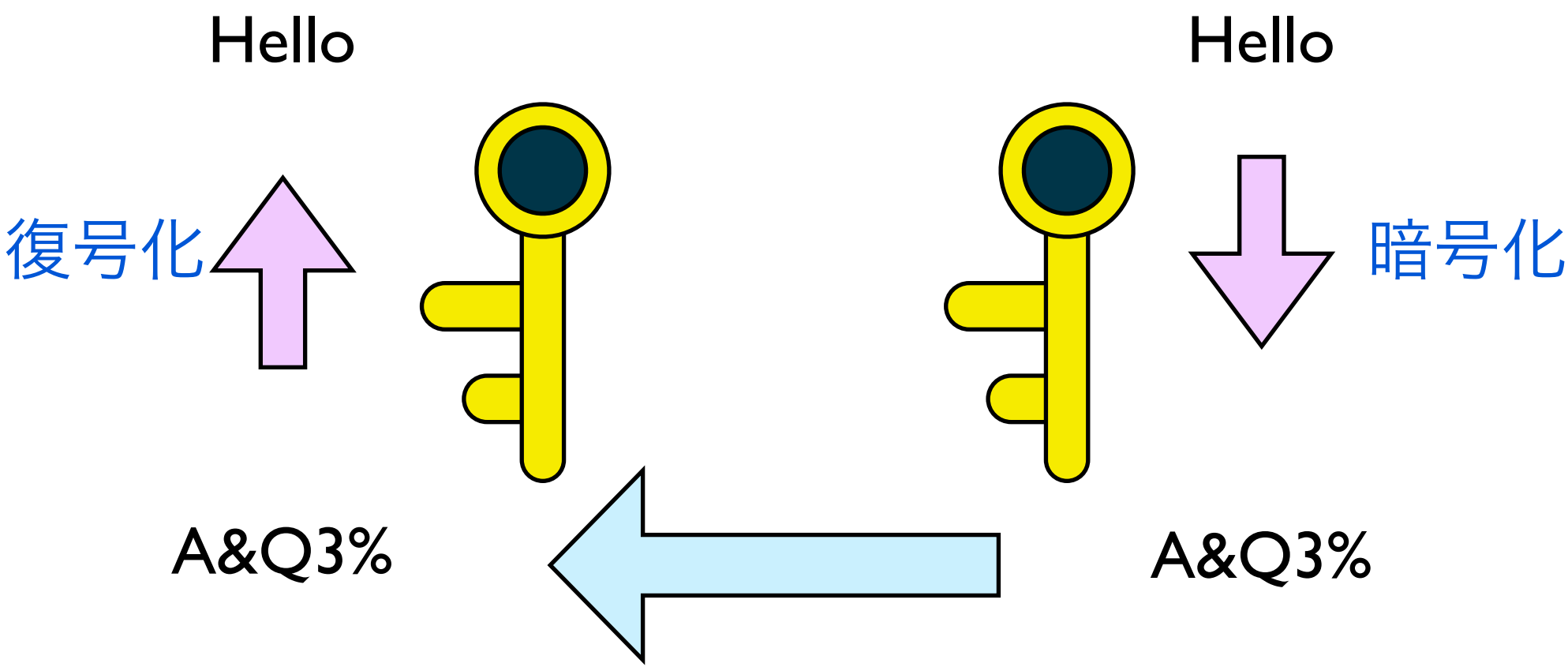
暗号化

- 共通鍵暗号
- 公開鍵暗号基盤 PKI (Public Key Infrastructure)
  - 公開鍵
  - 秘密鍵

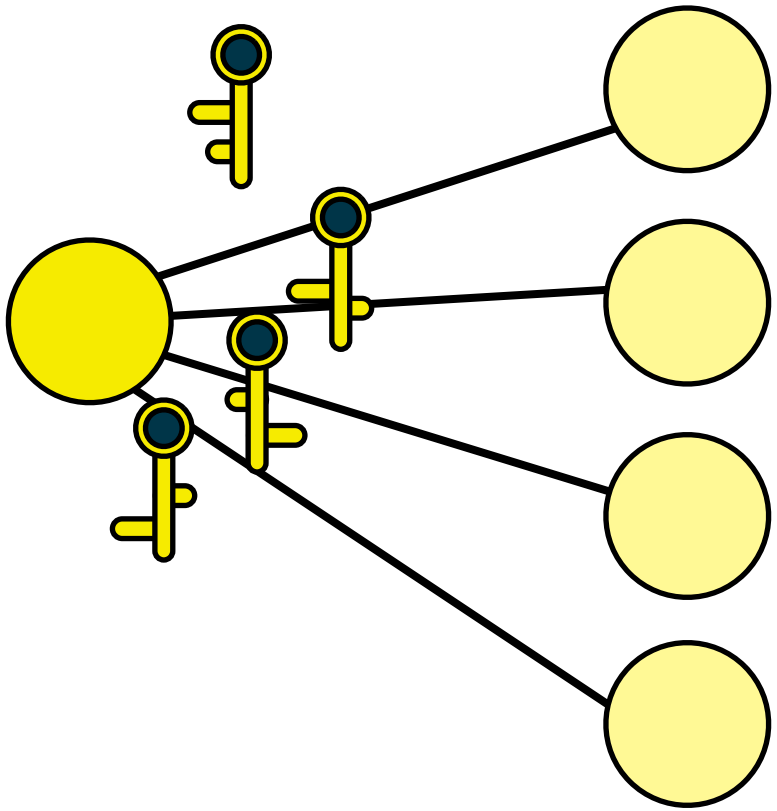
共通鍵暗号



共通鍵暗号

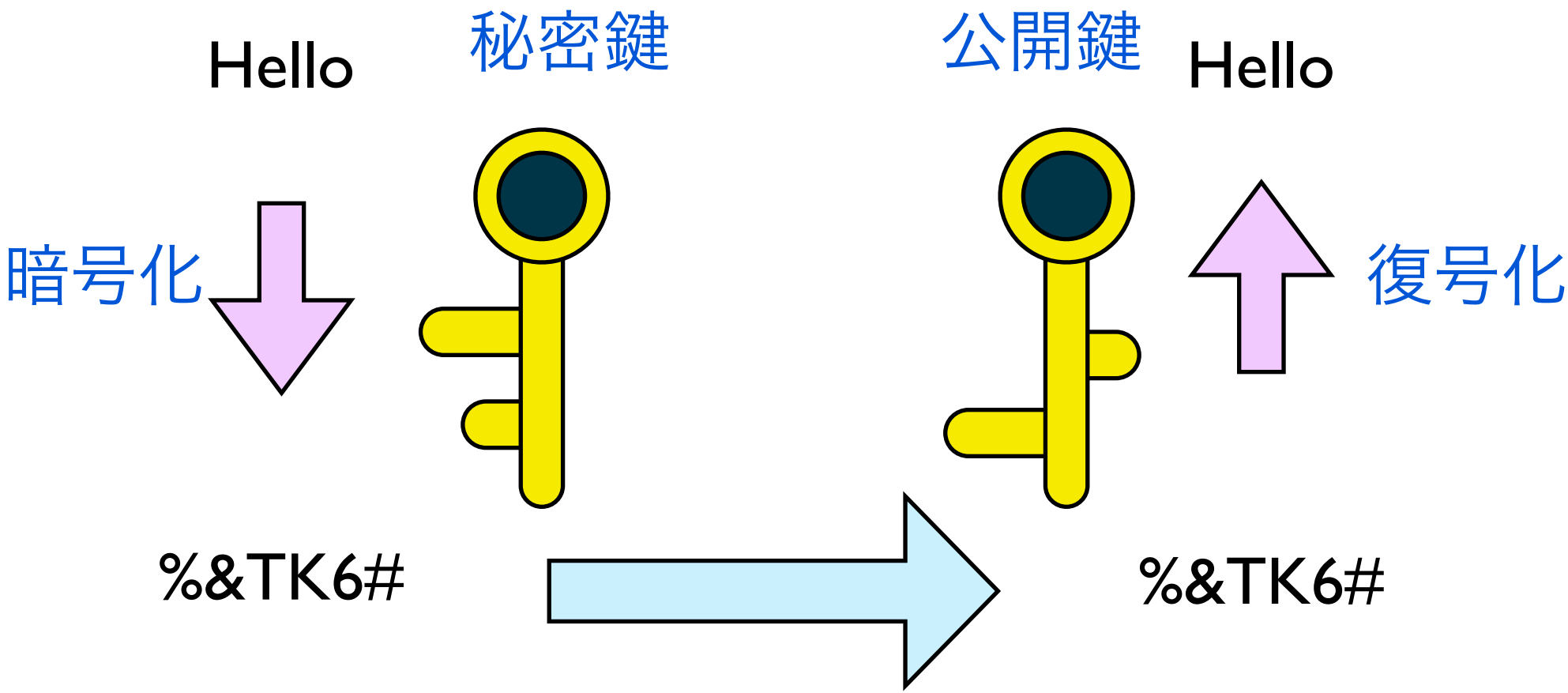


共通鍵の問題点

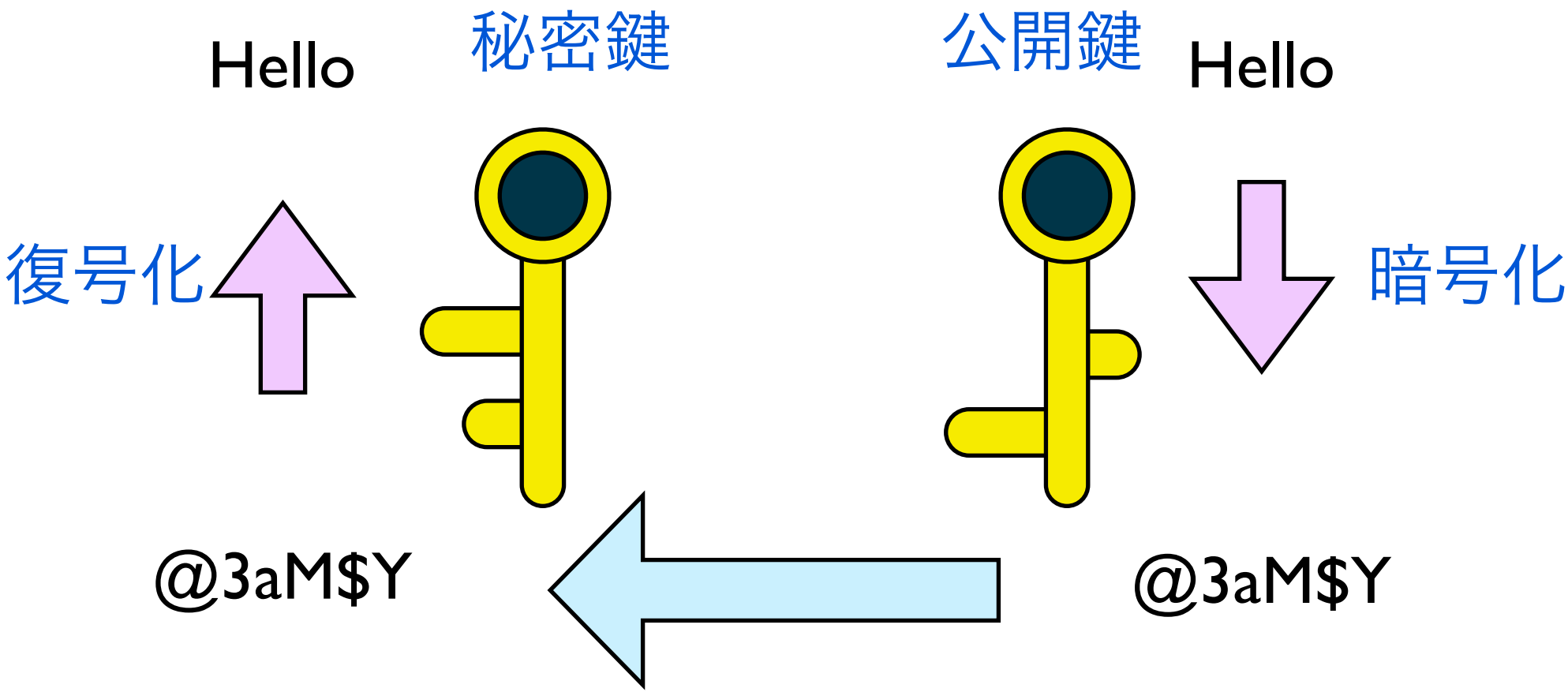


- 通信する相手ごとに鍵が必要
- 鍵の配布

公開鍵暗号



公開鍵暗号



電子署名

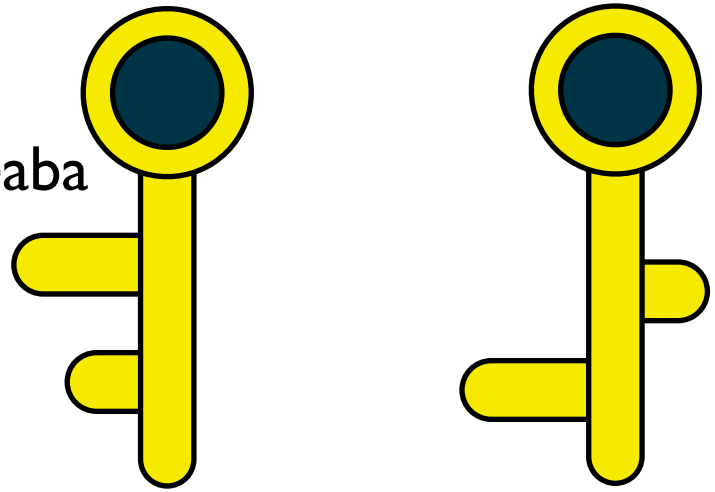
Hello, my friends

秘密鍵

公開鍵

Hello, my friends

ダイジェスト:Abe53f4aba



Abe53f4aba

比較

ダイジェスト

を暗号化

Abe53f4aba

署名を

復号化

Hello, my friends

Hello, my friends

署名: Bk@%&TK6#

署名: Bk@%&TK6#

電子署名

Hello, my friends

秘密鍵

公開鍵

Hello, your friends

ダイジェスト:Abe53f4aba

37cf2f4e8c

比較

ダイジェスト
を暗号化

Abe53f4aba

署名を
復号化

Hello, my fr nds

Hello, your friends

署名: Bk@%&TK6#

署名: Bk@%&TK6#